

1 **Claims**

2 What is claimed is:

3 1. A method comprising:

4 creating a data structure including a plurality of user id-user key pairs, each
5 user id-user key pair comprising a user id associated with one of a plurality of
6 users and a user key comprising a master key encrypted using a password
7 associated with the one of the plurality of users; and
8 delivering the data structure to one or more of the plurality of users.

9
10 2. A method as recited in claim 1, wherein the act of delivering
11 comprises delivering the data structure to each of the plurality of users.

12
13 3. A method as recited in claim 1, wherein each master key is
14 encrypted using a hash of the password associated with the one of the plurality of
15 users.

16
17 4. A method as recited in claim 1, wherein each master key is
18 encrypted using a one-way hash of the password associated with the one of the
19 plurality of users.

20
21 5. A method as recited in claim 1, wherein each master key is
22 encrypted using a cryptographic hash of the password associated with the one of
23 the plurality of users.

1 6. A method as recited in claim 1, wherein each user key has an
2 integrity verification feature associated therewith.

3
4 7. A method as recited in claim 1, wherein each master key has an
5 integrity verification feature associated therewith.

6
7 8. A method as recited in claim 1, wherein each master key and each
8 master key has an integrity verification feature associated therewith.

9
10 9. A method as recited in claim 1, wherein each user key includes a
11 checksum.

12
13 10. A method as recited in claim 1, wherein each user key includes a
14 keyed-hash message authentication code.

15
16 11. A method as recited in claim 1, further comprising:
17 transforming data using the master key.

18
19 12. A method as recited in claim 1, further comprising:
20 storing data transformed using the master key; and
21 controlling access by the plurality of users to the transformed data.

22
23 13. A method as recited in claim 1, further comprising:
24 storing data transformed using the master key;
25

1 receiving a user id and user password from one of the plurality of
2 users; and

3 controlling access to the transformed data by the one of the plurality
4 of users based on the received user id and user password.
5

6 14. A method as recited in claim 1, further comprising:
7 storing data transformed using the master key;
8 receiving a user id and user password from one of the plurality of
9 users; and
10 accessing the transformed data using the received user id and user
11 password.
12

13 15. A method as recited in claim 1, further comprising:
14 storing data transformed using the master key;
15 receiving a user id and user password from one of the plurality of
16 users;
17 selecting a user key from the data structure based on the received
18 user id;
19 decrypting the selected user id using the received password to
20 reproduce the master key; and
21 using the master key to access the data.
22

23 16. A method as recited in claim 1, further comprising:
24 storing data watermarked using the master key;
25

1 receiving a user id and user password from one of the plurality of
2 users; and
3 selecting a user key from the data structure based on the received
4 user id;
5 hashing the received password to produce a hash value;
6 decrypting the selected user id using the hash value to reproduce the
7 master key; and
8 using the master key to access the watermarked data.
9

10 17. A method comprising:
11 retrieving a user key associated with a first user of a plurality of
12 users from a data structure comprising a plurality of user keys, each user key
13 comprising a master key encrypted using a password associated with a unique one
14 of the plurality of users;
15 decrypting the retrieved user key using a password associated with
16 the first user to produce a master key; and
17 accessing data using the master key.
18

19 18. A method as recited in claim 17, wherein the user key is retrieved
20 using a user id associated with the first user.
21

22 19. A method as recited in claim 17, wherein the data structure
23 comprises a plurality of user id-user key pairs, each user id-user key pair
24 comprising a user id associated with one of a plurality of users and a user key
25 associated with the one of the plurality of users.

1
2 20. A method as recited in claim 17, wherein the data structure
3 comprises a plurality of user id-user key pairs, each user id-user key pair
4 comprising a user id associated with one of a plurality of users and a user key
5 associated with the one of the plurality of users, and wherein the user key is
6 retrieved using a user id associated with the first user.

7
8 21. A method as recited in claim 17, wherein the act of decrypting the
9 user key comprises decrypting the user key using a hash of the password
10 associated with the first user.

11
12 22. A method as recited in claim 17, wherein the act of decrypting the
13 retrieved user key comprises:

14 hashing the password associated with the first user to produce a hash value;
15 and
16 using the hash value as a decryption key to decrypt the user key.

17
18 23. A method as recited in claim 17, wherein the act of decrypting the
19 retrieved user key comprises:

20 hashing the password associated with the first user using a one-way hash
21 function; and
22 using the result of the one-way hash function as a decryption key to decrypt
23 the user key.

1
2 24. A method as recited in claim 17, wherein the act of decrypting the
3 retrieved user key comprises:

4 hashing the password associated with the first user using a cryptographic
5 hash function; and

6 using the result of the cryptographic hash function as a decryption key to
7 decrypt the user key.
8
9

10 25. A method as recited in claim 17, wherein each of the plurality of
11 user keys includes a data verification feature.
12

13 26. A method as recited in claim 17, wherein each of the plurality of
14 master keys includes a data verification feature.
15

16 27. A method as recited in claim 17, further comprising:
17 verifying the integrity of the retrieved user key.
18

19 28. A method as recited in claim 17, wherein the retrieved user key
20 includes an integrity verification feature and wherein the method further comprises
21 verifying the integrity of the retrieved user key using the integrity verification
22 feature.
23
24
25

1 29. A method as recited in claim 17, wherein the retrieved user key
2 includes a checksum and wherein the method further comprises verifying the
3 integrity of the retrieved user key using the checksum.

4
5 30. A method as recited in claim 17, wherein the retrieved user key
6 includes a message authentication code and wherein the method further comprises
7 verifying the integrity of the retrieved user key using the message authentication
8 code.

9
10 31. A method as recited in claim 17, wherein the retrieved user key
11 includes a keyed-hash message authentication code and wherein the method
12 further comprises verifying the integrity of the retrieved user key using the keyed-
13 hash message authentication code.

14
15 32. A computer readable medium having stored thereon a data structure
16 comprising:

17 a plurality of user id-user key pairs, each user id-user key pair comprising a
18 user id associated with one of a plurality of users and a user key comprising a
19 master key encrypted using a password associated with the one of the plurality of
20 users.

21
22 33. A computer readable medium as recited in claim 32, wherein each
23 user key comprises a master key encrypted using a hash of the password
24 associated with the one of the plurality of users.

1 34. A computer readable medium as recited in claim 32, wherein each
2 user key comprises a master key encrypted using a one-way hash of the password
3 associated with the one of the plurality of users.

4
5 35. A computer readable medium as recited in claim 32, wherein each
6 user key comprises a master key encrypted using a cryptographic hash of the
7 password associated with the one of the plurality of users.

8
9 36. A computer readable medium as recited in claim 32, wherein each
10 user key includes an integrity verification feature.

11
12 37. A computer readable medium as recited in claim 32, wherein each
13 master key includes an integrity verification feature.

14
15 38. A computer readable medium as recited in claim 32, wherein each
16 user key includes a checksum.

17
18 39. A computer readable medium as recited in claim 32, wherein each
19 user key includes a keyed-hash message authentication code.

20
21 40. A system comprising:
22 a hashing module operable to hash each of a plurality of user passwords
23 to produce a plurality of hash values;

1 an encryption module operable to create a plurality of user keys, each
2 user key comprising a master key encrypted using one of the hash values as an
3 encryption key; and

4 a data structure creation module operable to associate each of the user
5 keys with a user id in a data structure.

6
7 41. A system as defined in claim 40, wherein the hashing module
8 produces the hash values using a one-way hashing function.

9
10 42. A system as defined in claim 40, wherein the hashing module
11 produces the hash values using a cryptographic hashing function.

12
13 43. A system as defined in claim 40, wherein the data structure
14 creation module associates each user key with a user id in a user id-user key
15 pair, and wherein each user id-user key pair is associated with a single user.

16
17 44. A system as defined in claim 40, wherein the encryption module
18 includes an integrity verification feature in each user key.

19
20 45. A system as defined in claim 40, wherein the encryption module
21 includes a checksum in each user key.

22
23 46. A system as defined in claim 40, wherein the encryption module
24 includes a message authentication code in each user key.

1 47. A system as defined in claim 40, wherein the encryption module
2 includes a keyed-hash message authentication code in each user key.

3
4 48. A system comprising:
5 a user key data structure including plurality of user id-user key pairs,
6 each user key pair including a user key and a user id associated with one of a
7 plurality of users, each user key comprising an encrypted version of a common
8 master key;

9 a master key decryption module operable to select a user key from the
10 user key data structure based on a user id received from one of the plurality of
11 users and to decrypt the selected user key using a password received from the
12 one of the plurality of users.

13
14 49. A system as recited in claim 48, further comprising a data
15 decryption module operable to decrypt data encrypted using the master key as
16 an encryption key.

17
18 50. A system as recited in claims 48, further comprising an error
19 handler module operable to indicate to the one of the plurality when an error
20 occurs in decrypting the user key.

21
22 51. A system as recited in claims 48, wherein the master key
23 decryption module comprises:

24 a hashing module operable to hash a password received from the one of
25 the plurality of users to produce a hash value; and

1 a user key decryption module operable to select a user key from the user
2 key data structure based on a user id received from one of the plurality of users
3 and to decrypt the selected user key using the hash value as a decryption key.
4

5 52. A system as recited in claims 48, wherein the master key
6 decryption module comprises:

7 a hashing module operable to hash a password received from the one of
8 the plurality of users using a one-way hashing function to produce a hash value;
9 and

10 a user key decryption module operable to select a user key from the user
11 key data structure based on a user id received from one of the plurality of users
12 and to decrypt the selected user key using the hash value as a decryption key.
13

14 53. A system as recited in claim 48, wherein the master key
15 decryption module comprises:

16 a hashing module operable to hash a password received from the one of
17 the plurality of users using a cryptographic hashing function to produce a hash
18 value; and

19 a user key decryption module operable to select a user key from the user
20 key data structure based on a user id received from one of the plurality of users
21 and to decrypt the selected user key using the hash value as a decryption key.
22

23 54. A system as recited in claims 48, wherein the master key
24 decryption module comprises:
25

1 a hashing module operable to hash a password received from the one of
2 the plurality of users to produce a hash value; and

3 a user key decryption and integrity module operable to select a user key
4 from the user key data structure based on a user id received from one of the
5 plurality of users, to confirm the integrity of the selected user id, and to decrypt
6 the selected user key using the hash value as a decryption key.

7
8 55. A system as recited in claims 48, wherein each user key in the
9 user key data structure includes an integrity verification feature, and wherein the
10 master key decryption module comprises:

11 a hashing module operable to hash a password received from the one of
12 the plurality of users to produce a hash value; and

13 a user key decryption and integrity module operable to select a user key
14 from the user key data structure based on a user id received from one of the
15 plurality of users, to confirm the integrity of the selected user id using the
16 integrity verification feature included in the user key, and to decrypt the selected
17 user key using the hash value as a decryption key.

18
19 56. A system comprising:

20 means for producing a user key associated with each of a plurality
21 users, each user key comprising a master key encrypted using a password of the
22 one of the plurality of users associated with the user key;

23 means for associating each of the user keys with a user id of the one
24 of the plurality of users associated with the user key in a data structure.

1 57. A computer-readable medium having stored thereon computer
2 executable instructions for performing acts of:

3 creating a data structure including a plurality of user id-user key pairs, each
4 user id-user key pair comprising a user id associated with one of a plurality of
5 users and a user key comprising a master key encrypted using a password
6 associated with the one of the plurality of users.

7
8 58. A computer-readable medium as recited in claim 57 having further
9 computer executable instructions for performing acts of:

10 delivering the data structure to one or more of the plurality of users.

11
12 59. A computer-readable medium as recited in claim 57 having further
13 computer executable instructions for performing acts of:

14 delivering the data structure to each of the plurality of users.

15
16 60. A computer-readable medium as recited in claim 57, wherein each
17 master key is encrypted using a hash of the password associated with the one of
18 the plurality of users.

19
20 61. A computer-readable medium as recited in claim 57, wherein each
21 master key is encrypted using a one-way hash of the password associated with the
22 one of the plurality of users.

1 62. A computer-readable medium as recited in claim 57, wherein each
2 master key is encrypted using a cryptographic hash of the password associated
3 with the one of the plurality of users.
4

5 63. A computer-readable medium as recited in claim 57, wherein
6 each user key has an integrity verification feature associated therewith.
7

8 64 A computer-readable medium as recited in claim 57, wherein
9 each user key includes a checksum.
10

11 65. A computer-readable medium as recited in claim 57, wherein
12 each user key includes a keyed-hash message authentication code.
13

14 66. A computer-readable medium as recited in claim 57 having further
15 computer executable instructions for performing acts of:
16 transforming data using the master key.
17

18 67. A computer-readable medium as recited in claim 57 having further
19 computer executable instructions for performing acts of:
20 storing data transformed using the master key; and
21 controlling access by the plurality of users to the transformed data.
22

23 68. A computer-readable medium as recited in claim 57 having further
24 computer executable instructions for performing acts of:
25 storing data transformed using the master key;

1 receiving a user id and user password from one of the plurality of
2 users; and

3 controlling access to the transformed data by the one of the plurality
4 of users based on the received user id and user password.
5

6 69. A computer-readable medium as recited in claim 57 having further
7 computer executable instructions for performing acts of:

8 storing data encrypted using the master key;
9 receiving a user id and user password from one of the plurality of
10 users; and

11 accessing the transformed data using the received user id and user
12 password.
13

14 70. A computer-readable medium as recited in claim 57 having further
15 computer executable instructions for performing acts of:

16 storing data encrypted using the master key;
17 receiving a user id and user password from one of the plurality of
18 users;

19 selecting a user key from the data structure based on the received
20 user id;

21 decrypting the selected user id using the received password to
22 reproduce the master key; and

23 using the master key to decrypt the data.
24
25

1 71. A computer-readable medium as recited in claim 57 having further
2 computer executable instructions for performing acts of:

3 storing data watermarked using the master key;
4 receiving a user id and user password from one of the plurality of
5 users; and
6 selecting a user key from the data structure based on the received
7 user id;
8 hashing the received password to produce a hash value;
9 decrypting the selected user id using the hash value to reproduce the
10 master key; and
11 using the master key to access the watermarked data.
12

13 72. A computer-readable medium having stored thereon computer
14 executable instructions for performing acts of:

15 retrieving a user key associated with a first user of a plurality of users from
16 a data structure comprising a plurality of user keys, each user key comprising a
17 master key encrypted using a password associated with a unique one of the
18 plurality of users;
19

20 decrypting the retrieved user key using a password associated with
21 the first user to produce a master key; and

22 accessing data using the master key.
23

24 73. A computer-readable medium as recited in claim 72, wherein the
25 user key is retrieved using a user id associated with the first user.

1
2 74. A computer-readable medium as recited in claim 72, wherein the
3 data structure comprises a plurality of user id-user key pairs, each user id-user key
4 pair comprising a user id associated with one of a plurality of users and a user key
5 associated with the one of the plurality of users.
6

7 75. A computer-readable medium as recited in claim 72, wherein the
8 data structure comprises a plurality of user id-user key pairs, each user id-user key
9 pair comprising a user id associated with one of a plurality of users and a user key
10 associated with the one of the plurality of users, and wherein the user key is
11 retrieved using a user id associated with the first user.
12

13 76. A computer-readable medium as recited in claim 72, wherein the act
14 of decrypting the user key comprises decrypting the user key using a hash of the
15 password associated with the first user.
16

17 77. A computer-readable medium as recited in claim 72, wherein the act
18 of decrypting the retrieved user key comprises:

19 hashing the password associated with the first user to produce a hash value;

20 and

21 using the hash value as a decryption key to decrypt the user key.
22
23
24
25

1
2 78. A computer-readable medium as recited in claim 72, wherein the act
3 of decrypting the retrieved user key comprises:

4 hashing the password associated with the first user using a one-way hash
5 function; and

6 using the result of the one-way hash function as a decryption key to decrypt
7 the user key.
8

9 79. A computer-readable medium as recited in claim 72, wherein the act
10 of decrypting the retrieved user key comprises:

11 hashing the password associated with the first user using a cryptographic
12 hash function; and

13 using the result of the cryptographic hash function as a decryption key to
14 decrypt the user key.
15

16 80. A computer-readable medium as recited in claim 72, wherein each of
17 the plurality of user key includes a data verification feature.
18

19 81. A computer-readable medium as recited in claim 72 having further
20 computer executable instructions for performing acts of:

21 verifying the integrity of the retrieved user key.
22

23 82. A computer-readable medium as recited in claim 72, wherein the
24 retrieved user key includes an integrity verification feature and wherein the
25

1 method further comprises verifying the integrity of the retrieved user key using the
2 integrity verification feature.

3
4 83. A computer-readable medium as recited in claim 72, wherein the
5 retrieved user key includes a checksum and wherein the method further comprises
6 verifying the integrity of the retrieved user key using the checksum.

7
8 84. A computer-readable medium as recited in claim 72, wherein the
9 retrieved user key includes a message authentication code and wherein the method
10 further comprises verifying the integrity of the retrieved user key using the
11 message authentication code.

12
13 85. A computer-readable medium as recited in claim 72, wherein the
14 retrieved user key includes a keyed-hash message authentication code and wherein
15 the method further comprises verifying the integrity of the retrieved user key using
16 the keyed-hash message authentication code.